AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

Science, Technology, Engineering and Mathematics (STEM): Mandating an Education Quota in the USAF Intelligence, Surveillance and Reconnaissance (ISR) Officer Corps

by

Matthew P. Bruno, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Mr. Michael P. Ivanovsky and Major Cashenna A. Cross

Maxwell Air Force Base, Alabama

February 2013

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

Abstract

This paper analyzes literature pertaining to USAF's Intelligence, Surveillance and Reconnaissance (ISR) professionals and the connection with Science, Technology, Engineering and Mathematics (STEM) education. Also, the research delves into USAF cyberspace structure, forces and risks. The focus is gleaned from respected sources and DoD and USAF Directives, Guidance and Doctrine referencing cyber, ISR, STEM and education. Accordingly, this paper explores the topics of USAF's goals; current response and possible way ahead to grow a STEM educated ISR professionals in several steps. The first is to summarize the current operating environment within cyberspace. The second is to define how the US Government and DoD are emphasizing STEM education. The third is to interpret the USAF cyberspace force structure. The fourth is to explain the Air Force's approach to STEM. The fifth will quickly cover the risks facing the Air Force. The six proposes a solution and drawbacks. The seventh and final section will summarize the research and provide recommendations for further research.

Who should the USAF target and then further develop as Cyber ISR professionals? For cyberspace, an ever increasing number of Airmen must have the proper background, education and training anchored in STEM to be agile, innovative and successful. To grow a dynamic workforce and meet the ever growing challenges within cyberspace, the USAF must set a quota for STEM educated Airmen and steadily increase it for accessions and cross-flows into the Intelligence (14N) career field. In light of lower manning and budgets, the USAF must recruit and retain 14Ns with STEM degrees today to succeed in the future. By immediately instituting a twenty-percent quota for STEM education as a prerequisite for the 14N career field, the USAF will meet the current percentage of 14Ns working in positions directly supporting or supported by cyber operations and be better positioned for future success.

Science, Technology, Engineering and Mathematics (STEM): Mandating an Education Quota in the USAF Intelligence, Surveillance and Reconnaissance (ISR) Officer Corps

Introduction

With the creation of US Cyber Command (USCYBERCOM) and associated service components, it is increasingly evident the US has a focus and execution arm within cyberspace. In his work, *Cyber Power*, Joseph Nye states, "America's 10th Fleet and 24th Air Force have no ships or planes; their battlefield is cyberspace."[1] The US is in the process of building and honing its capacity for cyber operations through USCYBERCOM and various governmental agencies such as the Department of Homeland Security, which is the lead for non-DoD networks. The designation of the lead agency depends on the physical network, authorities and type of action. At this time, USCYBERCOM, a sub-unified command under USSTRATCOM, is the lead for DoD networks and Title 10 authorities within cyberspace.[2] This paper will not expound on the legal issues, policy challenges and authority divisions within the US Government.

What is essential to success in cyberspace? While physical infrastructure, machines and associated technology are important, the workforce is the critical element. USCYBERCOM must have a well-trained, educated, credible and competent cyber workforce. The service components are responsible for providing, equipping and training forces. Recently, the USAF has signaled the importance of cyberspace by incorporating it as a domain into its mission statement.[3] In his work, *Cyber Vision and Cyber Force Development*, Doctor Kamal Jabbour states, "By adding cyberspace to its mission statement and standing up a cyber-space command, the USAF took on the challenge to develop and present forces ready to fight in this domain.[4]

To *fly, fight and win* within the complex domain, the 24th AF and other USAF units will rely heavily on Intelligence, Surveillance, and Reconnaissance (ISR) professionals, who provide

accurate, timely and relevant information to decision makers.[5] Cyber ISR strives for key knowledge of friendly and enemy networks and threat actors in order to conduct operations within cyberspace.[6] As with the traditional domains, ISR professionals strive to develop a timely and accurate Intelligence Preparation of the Operating Environment (IPEO) picture to drive operations. Due to the complexity and challenges of the domain, some consider Cyber ISR or Cyber Intelligence (CYBINT) a new branch or discipline of intelligence. Jabbour argues CYBINT focuses on both sides in a conflict while traditional IPOE tends to focus only on the enemy.[7] Regardless of terminology and labels, the USAF must provide a capable cadre of ISR professionals who can navigate and operate within cyberspace. These professionals must produce indications and warning, define threats and challenge false paradigms, which are the purposes of Intelligence.[8]

Who should the USAF target and then further develop as Cyber ISR professionals? The cyberspace savvy ISR professionals must have the proper background, education and training anchored in Science, Technology, Engineering and Mathematic (STEM). There is little dispute effective cyber operations require a well-educated, developed and trained workforce.[9] Jabbour posits cyber warriors must have a STEM background and should hold a computer or electrical engineering degree, which provides a necessary foundation as well as prepare them for the unknown challenges of the future.[10] To grow a dynamic workforce and meet the ever growing complexity within cyberspace, the USAF must set a twenty-percent quota for STEM educated Airmen and steadily increase it for accessions and cross-flows into the 14N career field. The problem is the Air Force Personnel Management System and structured programs do not provide enough officers with the educational background, breadth and depth of knowledge and experience in cyberspace. The current assignment, accession, training and education model does

not produce enough leaders with STEM capabilities nor degrees.[11] In light of lower manning and budget levels, the USAF must recruit and retain 14Ns with STEM degrees who will be better prepared today to succeed in the future. In the words of General Walter Givhan, "This new war-fighting domain needs enormous amounts of STEM investment at all ranks and at all levels."[12] Cyber ISR war-fighters built from STEM education have the necessary background to be agile, innovative and successful within cyberspace. By immediately instituting a twenty percent quota for STEM education as a prerequisite for the Intelligence career field, the USAF will be better positioned for future operational success. Currently, twenty-one percent of USAF 14Ns work in positions supporting or supported by cyberspace operations.[13] Thus, instituting a twenty-percent quota, identified in figure 1, meets current demands in cyberspace, Signals Intelligence (SIGINT), Targeting and Space.[14]

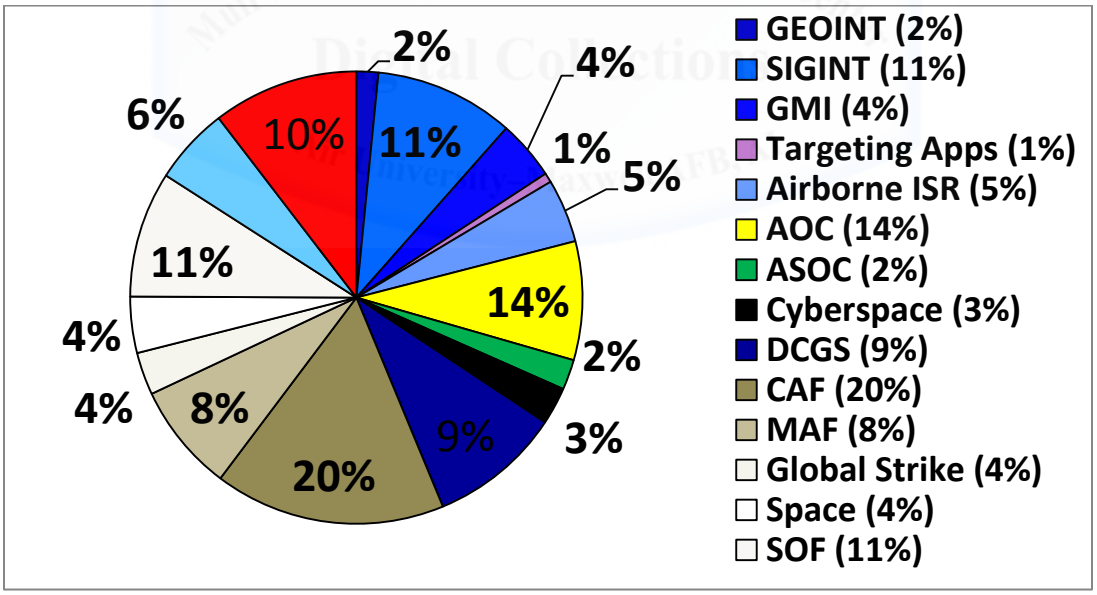

Figure 1. CGO 14N Utilization

This paper analyzes literature pertaining to USAF's ISR professionals and the connection with STEM education. Also, the research delves into USAF cyberspace structure, forces, training, skills, available personnel and partnerships, all of which impact USAF's

intentions and approach to this domain. The focus is gleaned from respected sources and DoD and USAF Directives, Guidance and Doctrine referencing cyber, ISR, STEM, training and education. Accordingly, this paper explores the topics of USAF's goals; current response and possible way ahead to grow a STEM educated ISR professionals in several steps. The first is to summarize the current operating environment within cyberspace. The second is to define how the US Government and DoD are emphasizing STEM education. The third is to interpret the USAF cyberspace force structure. The fourth is to explain the Air Force's approach to STEM. The fifth will quickly cover the risks facing the Air Force. The six proposes a solution and possible drawbacks. The seventh and final section will summarize the research and provide recommendations.

Cyberspace Operating Environment

At times, it is easy to forget just how new the cyber domain is. What is difficult to ignore is the complexity and technical challenges of the domain. Much has been and continues to be written on the challenges and issues associated with cyberspace. Cyberspace as an operational domain is framed by the use of electronics to store, modify, exploit and exchange information via interconnected systems and their associated physical infrastructure.[15] In contrast to the domains of land, sea, air and space, cyberspace is man-made and in some aspects only limited by human imagination.[16] Currently, a magnitude of ambiguous actors, varied threats, insecurity, lack of attribution and unclear legal guidelines dominate this domain. Due to these factors, the execution of cyber operations, to include ISR support, remains very challenging and requires technically educated and competent professionals.

The cyberspace domain is full of vulnerabilities and subsequent losses of security and data. Unfortunately, vulnerabilities and losses are well beyond the private user and have the

potential to adversely impact the entire country.[17] In his work on cyber operations, Stephen Korns writes, the US Department of Defense (DOD) has lost terabytes of data equivalent to twice the holdings of the Library of Congress.[18] Since the USAF is reliant on technology, values innovation and strives for information superiority, this trend is quite concerning. The USAF should better build and posture their ISR professionals with backgrounds in STEM. As in the other domains, ISR professionals often identify who and the why behind events. To increase cyber security, nations respond with a combination of law enforcement, military and intelligence operations.[19] Depending on the event, threat and associated actor, USAF ISR professionals could be involved in any of these aspects.

US Government and DoD STEM Approach

Throughout the *2010 National Security Strategy (NSS)*, the White House stresses education, science, technology and innovation as essential elements to US strength, prosperity and long term competitiveness.[20] The *2011 DoD Strategy for Operating in Cyberspace* emphasis education and training as the hallmarks for the cyber workforce and development of the government's intellectual capital.[21] Unfortunately, the US suffers from a shrinking pool of STEM educated personnel as other counties graduate more scientists and engineers than the United States.[22] For the US, the shortages in appropriately educated personnel are the result of three factors: 1) a dramatic increase in dependency on technology, 2) the retirements of the "baby boom" generation and 3) declining interest in STEM by US students.[23] Both the DoD and Intelligence Community (IC) have an increasingly difficult time filling positions in engineering, forensics, computing and other STEM disciplines. As a result, the DoD has taken many steps to attract and develop STEM education professionals. For example, the *DoD STEM Education and Outreach Strategic Plan* brought together ninety experts to create a plan to: 1) develop a

systematic approach for education and outreach, 2) provide an accessible inventory of programs and 3) implement a communications strategy.[24] Also, one of the five strategic goals within the *DoD Strategy for Operating in Cyberspace* is to develop the workforce and be competitive to attract technically skilled personnel to join government for the long-term.[25]

USAF Cyber Force Structure

For the USAF, many different career fields, operational roles and technical skill sets comprise the cyber workforce. In 2010, the 17D and 3DX Officer and Enlisted Air Force Specialty Codes (AFSC) were activated and designated as the USAF's cyberspace operators.[26] Thus, the 17D, associated enlisted and civilian workforce form the bulk of the cyberspace team and receive the majority of the related training and advanced education. USAF leadership and the managers of 17Ds recognize there is a need for a STEM educated cyber force. Based on current skill set requirements, fifty percent of cyber officers (17Ds) hold STEM degrees.[27] Of these only twenty-five percent are directly related to cyberspace.[28] Also, approximately sixty-five percent of the cyber force is enlisted where undergraduate degrees are not required. In addition, based on the occupational series, civilians may or may not have STEM degree requirements. In 2011, the core USAF Cyber warriors consisted of nineteen separate Officer, Enlisted and Civilian career fields.[29] In 2012, this number was expanded to twenty-two with the inclusion of the Office of Special Investigations.[30] This signals the importance of Counter-Intelligence and Human Intelligence (HUMINT) as cyber war-fighting skills. Of note, other career fields such as the Staff Judge Advocates who increasingly contribute to the cyber mission are not included in the core cyber workforce.

To develop Cyberspace professionals and the necessary critical skills, Air Force Space Command (AFSPC) has been designated as the functional lead.[31] As the lead MAJCOM,

AFSPC organizes, trains, and equips (OT&E) Air Force cyberspace forces for USCYBERCOM through the 24th AF, associated units and other Airmen.[32] In 2012, AFSPC proposed designating six capabilities such as cyberspace defense analysis as weapon systems in accordance with their OT&E mission.[33] 24th AF is the hub for cyberspace operations and manning. However, the USAF also presents forces to the IC, which executes different mission sets or receives data from cyberspace.

As a core component of the cyber force, the USAF Intelligence Officer (14N) and associated enlisted and civilian carrier fields are vital to cyber operations. In the *Air Force Roadmap for the Development of Cyberspace Professionals*, it is imperative ISR professionals provide commanders with battlespace awareness and technical intelligence as well as have the capability to conduct and support operations in cyberspace.[34] To leverage all ISR disciplines, Intelligence professionals must have an extensive understanding of the cyberspace domain.[35] As the USAF Service Cryptologic Component to the National Security Agency / Central Security Service, the Air Force Intelligence, Surveillance and Reconnaissance Agency (AFISRA) is responsible for the execution of the Signals Intelligence (SIGINT) mission and designated USAF led ISR missions, vital to cyberspace operations.[36] Also, AFISRA, a Direct Reporting Unit under Headquarters Air Force Director of Intelligence (HAF/A2), is responsible for the development of ISR professionals. Overall the management and force development of ISR career fields are handled between the HAF/A2 and the Air Force Personnel Center (AFPC). As Lieutenant General Larry James, HAF/A2, recently stated, "Operations in cyberspace are indivisible from ISR because, in cyber, there is a tremendous demand to simultaneously understand and exploit vulnerabilities to enable operations."[37] General James argues the USAF must continue to invest talent and resources into the integration of cyber with air and space.[38]

AFISRA recently stood-up the new 659th ISR Group to provide direct ISR support to the 24th AF, which contributes to the USCYBERCOM mission. While debate continues to evolve on the proper structure for Air Force ISR, what is clear is that ISR professionals will continue to strengthen linkages and integration with cyber, electronic warfare and information operations.[39]

USAF STEM Approach

How is the USAF emphasizing and incorporating STEM into the cyber workforce? In her 2012 testimony to congress, Major General Suzanne Vautrinot, Commander 24th AF, posited a proper foundation, which starts with early exposure to STEM, is critical to building a strong structure.[40] The stated goal of *Bright Horizons*; *The Air Force STEM Strategic Roadmap*, is to shape the way the USAF manages the mission critical capabilities, which achieve and assure a war-fighting edge.[41] The document also calls for the establishment of yearly STEM accession goals for the USAF Academy, ROTC and OTS.[42] Due to the high percentage of STEM designated positions, career field managers of Space and Missile (13S) and 17Ds are considering instituting hard quotas.[43] Excluding the medical corps, nine USAF Officer Career fields consisting of Experimental Test Pilots (11E), Experimental Weapons Systems Officers (12E), Astronauts (13A), Civil Engineers (32E), Research Analysts (61A), Scientists (61B), Physicists (61C), Physicists (61D), and Developmental Engineers (62E) have STEM degree requirements for accessions.[44] However, at this time, the 14N career field does not have a minimum STEM requirement.

In *Flying and Fighting in Cyberspace*, Lieutenant Colonel Sebastian Convertino argues for a requirement for cyber related education prior to entry into service, and mission-specific training before cyber recruits participate in operations.[45] In 2007, Convertino further identified the need for heavy USAF investments to include increased recruiting from colleges of STEM

educated students, providing scholarships and research grants, and proposing special retention bonuses and the creation of a separate pay scale for civilian cyber experts.[46] While some may view these initiatives as excessive the USAF has gradually increased scholarships, training and advanced education to meet current demands. In 2000, USAF leadership identified a critical shortfall in STEM manning and instituted manpower requirements, processes and increased funding, which require review, further refinement and increased emphasis.[47]

How is the USAF expanding advanced education and training programs for cyberspace? The Air Force Institute of Technology (AFIT) provides training and advanced technical and cyber related degrees. AFIT along with the Air Force Research Laboratory (AFRL) are the main sources for Air Force STEM personnel, research and education.[48] Also, the AFIT Advanced Academic Degree (AAD) and Special Experience Exchange Duties (SPEED) program, provides opportunities for multiple career fields to obtain advanced technical degrees.[49] Currently, there are ten recognized foundational, continuing or advanced training courses executed through five organizations which include AFIT and the USAF Weapons School.[50] To understand the importance of formal STEM education and advanced opportunities the Air Force needs to distinguish between education and training. Training provides Airmen with proficiency to operate current tools, whereas education builds a foundation that prepares professionals to deal with unknown future challenges.[51] For the USAF, most of the cyber training courses are built for 17Ds and Intelligence Officers attend the training and educational courses if they meet the prerequisites and are filling positions providing support to or from cyberspace. There is also Intelligence Officer specific training for cyber, but this is minimal. For example, 14Ns only receive two-days of cyber training at the Basic Intelligence Officer Course, Goodfellow Air

Force Base.[52] This paper does not discuss the training and educational opportunities offered outside of the USAF.

The Risks Facing the USAF

As noted, there is an identified need to increase STEM education in the cyber workforce along with major efforts by the DoD and USAF to increase STEM accessions. A basic understanding of the operating environment helps explain the risks the USAF will face if they fail to increase the number of STEM educated ISR officers. A review of the literature reveals three primary risks; 1) inability to operationalize cyberspace, 2) forfeiture of technical edge and 3) loss of "Airmindedness".

The first risk is the USAF's inability to operationalize the cyberspace domain. While having no other purpose than to serve humans, this domain is connected to and causes effects within the physical world, which can create effects in the air and space domains.[53] Operations in cyberspace can create effects in the other domains such as air and space. The speed of cyberspace events is unlike the other domains, and occurs at the speed of byte or two-thirds the speed of light.[54] Martin Libicki, notable author on cyberspace, notes, the time between launch of an attack and its effects is barely measurable, thus creating instantaneous risks for decision makers.[55] Traditionally, the USAF has stressed and utilized global reach and speed to execute operations. The USAF must build greater capacity and skill within the Cyber ISR workforce to generate sustainable operational capabilities and integrate them into air and space operations.[56] If unable to execute independent cyber operations, USAF Airmen and its ISR professionals will be regulated to a junior workforce within other government agencies.

The second risk is the forfeiture of the USAF's technical edge. Technical prowess, ingenuity, and an ability to adapt and overcome challenges are hallmarks of USAF Airmen.[57] For

example, scientific developments such as Global Positioning Satellites and stealth technology have increased the range, versatility and effectiveness of USAF operations. Throughout the NSS, the White House stresses the goals of protecting our information, communication, critical infrastructure and intellectual property.[58] As Lieutenant Colonel Dean Clothier, Commander 39th Information Operations Squadron posits, of the services the USAF is the furthest along in the cyber enterprise, because the risk is highest.[59] Due to our reliance on technology and innovation, the Air Force has the most to lose amongst the service components. A prime example is when malicious actors steal intellectual data for design of the F-22, a critical future weapon system.

The third risk facing the USAF is loss of ISR and associated data from cyberspace pertinent to air and space operations, which Airmen care about. The US Air Force has developed an enduring culture and unique personality driven by *Airminded* Airmen. Prior to WWII, General Billy Mitchell, an airpower pioneer, argued for a new class of *air-going people* with a distinct spirit, language and belief for air.[60] In AFDD-1, *Airmindedness*, the perspective of Airmen is necessarily different; it reflects a unique appreciation of airpower's potential, as well as the threats and survival imperatives unique to Airmen.[61]

At the national level, intelligence resources are finite and in high demand, and USAF requirements which are not always a high national priority may go unfulfilled. To provide for service specific requirements the USAF has designated the National Air & Space Center (NASIC), a center of excellence and hub of STEM educated Airmen.[62] NASIC provides scientific, technical and general military intelligence and analysis regarding foreign Air and Space capabilities. The Air Force has recently began to reinvest in a HUMINT force, which signals the growing demand for ISR data necessary to accomplish USAF specific mission sets. The USAF requires an organic CYBINT capability to focus on what Airmen care about in

cyberspace. Without a capable and credible workforce that can synergize effects across air, space and cyberspace, the Air Force risks failure in future operations.

Solution and Drawbacks:

Cyberspace is a mix of ISR and operations. The USAF increasingly relies on ISR professionals with highly technical degrees to meet the challenges of cyberspace and adapt with greater agility. In cyberspace, there is no substitute for a talented well-educated and trained workforce. The development of Cyber ISR professionals with STEM education will ensure the USAF has the ability to *Fly, Fight and Win* in cyberspace. Air Force leaders and intelligence professionals must recognize persistent ISR as a critical requirement for air, space, and cyberspace operations—not just air.[63] Along with the USAF recognizing new technologies and leveraging innovative capabilities, the future development of Cyber ISR professionals must be a significant part of the service's strategy.[64]

How is the USAF Intelligence community currently addressing STEM needs? USAF leadership and managers of the Intelligence career field understand the importance of STEM. In the recent cross-flow board, the assignments team requested Airmen with STEM education and cyberspace.[65] Also, HAF/A2 ISR Force Management recently published a new Career Field Education and Training Plan stating, "The highly technical nature of ISR requires equally technical expertise (particularly in cyber and computer topics). Any degrees in the science, technology, engineering and mathematics (STEM) fields are useful for intelligence officers. The dependence of intelligence on sound data management and evaluation makes degrees in operations research, statistics, accounting, and other hard sciences valuable."[66] The current Air Force Classification Directory (AFOCD) calls for undergraduate specialization or degrees in physical, earth, computer, social or information sciences, engineering, mathematics, or foreign

area studies for 14Ns. The Air Force will soon publish a new AFCOD which strengthens, but does not mandate a STEM educational requirement for the 14N career field.[67]

Air Force leadership must fulfill its requirements as a force provider, and bolster STEM educated personnel to meet the challenges in cyberspace. The USAF must take strong steps to include an immediate institution of a twenty percent quota for new accessions or cross-flows into the 14 career field. Currently, nine percent of USAF Intelligence Officers work in positions specified as Cyberspace, Space and Targeting, and eleven percent are assigned to Signals Intelligence (SIGINT) positions.[68] The base number of twenty percent simply equates to current STEM demands as depicted in *Figure 1, CGO 14N Utilization*. As STEM educated personnel requirements increase, the USAF personnel system should correspondingly increase the quota to a sustainable or achievable rate. At the moment the AFCOD states STEM related degrees are desirable, but without setting a hard quota, career field managers missing the chance to proactively meet the requirement before it becomes critical. Other career fields have set or are considering hard quotas for specific degrees.

Cyber Vision 2025 calls for the Air Force to change the current classification guide to ensure a minimum of 50 percent of accessions to the 17D career field to have a cyber-specific degree.[69] It takes ten years to develop a Major and fifteen years to groom a Lieutenant Colonel. The time to act is now! As General Patton states, "A good plan violently executed now is better than a perfect plan executed next week." Without transformation, USAF Intelligence will be incapable of supporting the full range of operations in cyberspace and exploit key information in this domain. Further refinement of the Air Force specialty code-awarding criteria and graduate level cyber courses must continue to rank high among the top priorities for the USAF.[70]

The USAF should continue leveraging existing schools within the DoD, IC, public and private institutions to advance the number of STEM educated personnel. Also, the USAF should validate training standards and develop relevant Knowledge Skills and Abilities (KSAs) criteria for CYBINT analysts. The USAF must identify, fund, and steer ISR professionals towards STEM degrees in computer science and information assurance. Sustaining this force requires a commitment of tough manpower choices and management of assignments. For example, ROTC scholarships could be increasingly linked to STEM degrees. If students decide to change majors to a non-STEM degree then they could lose their scholarship. Convertino argues, "In order to be truly effective within cyberspace, the Air Force will have to adapt to accept increased numbers of unconventional warriors.[71] Also, Officer Training School (OTS) could be restricted to those aspiring officers who hold technical degrees. General Givhan states, "Military organizations, however, must grow their own."[72] The Air Force can control funding and program selection for OTS, USAF Academy and AFIT accessions and ROTC scholarships could be increasing linked to STEM.

Despite the challenging fiscal environment the USAF should implement a critical skills retention bonus (CSRB) for STEM educated Officers holding Advanced Academic Degrees. This bonus would remain in effect until the USAF improves sustainment numbers in career fields which require increased numbers of qualified personnel with the proper STEM background. Despite the lack of mandate in the 14N career field, a bonus would target officers with four to ten years of commissioned service. Recently, the career field managers pushed for a bonus for all 14N officers within those year groups.[73] This author believes bonuses should be tailored to STEM educated personnel who can help meet today's complex threats and technical challenges.

However, research indicates three potential drawbacks or common arguments against setting a STEM quota; 1) conflicting and competing requirements in ISR, 2) shortage of STEM educated personnel and 3) potential adverse impact to diversity. There is a large spectrum of functions and shifting priorities within the Air Force Intelligence Officer's area of responsibility, making it difficult to determine the ideal breakdown of education and training. The USAF ISR community must drive toward implementation of more "rigor" in the development of Cyber ISR professionals. Recently, HAF/A2 implemented a Career Path Tool to more aggressively track depth and breadth of experience, training and education gained in the different Intelligence career paths.[74] As a community, ISR has many moving parts and competing requirements, but it must continue to move forward.

Secondly, the US Government as a whole suffers from a STEM shortage. Only seven percent of USAF officers hold degrees in computer and electrical engineering, which provides a solid foundation for the cyber officer corps.[75] There are USAF programs in place designed to increase student interest in STEM, to include AFIT's Advanced Cyber Education (ACE) program for ROTC cadets from all services and the Air Force Association's Cyber Patriot program. In the mid-term of five to ten years, numbers of STEM educated Airmen can be bolstered by increased funding and management of programs at AFIT, OTS, ROTC and the USAF Academy. Also, the USAF should increase slots for STEM degrees while reducing slots for non-technical degrees.

The third argument for not implementing quotas is the potential negative effects on diversity. Women and minorities continue to be underrepresented in STEM.[76] However, the argument for diversity bases on gender and race alone should not guide the pace of evolution nor place the USAF at an operational disadvantage. At all levels of the US Government, to include

the USAF, many initiatives engage and attempt to bolster US student interest and continue to emphasize STEM in underrepresented and underprivileged areas.[77] Despite these challenges, the USAF must meet the requirements because the risk of mission failure is too great. The USAF cannot wait fifteen years to develop a relevant cyber-vision and a competent Cyber ISR workforce.

Conclusion

The complex and challenging environment of Cyberspace requires well educated and trained ISR professionals. Not every Airman can be expected to hold a STEM related degree despite the need for these specialists is soaring at an ever increasing rate. Without STEM educated Airmen, the Air Force will become a delegated junior workforce, continue to lose its technical edge and eventually fail to meet service requirements and national security demands as outlined by top US leadership. The Air Force must incorporate STEM into ISR as one of its most urgent priorities. An immediate twenty–percent quota for STEM degrees for accessions in the 14N career field would be a start. The pace of change in cyberspace demands an increased combination of technology and human innovation to enhance Air Force Cyberspace operations and optimize effectiveness.

Although much progress has been made in recent years, uncertainty exists at the highest levels as to what exactly comprises the USAF's operational role and force provider responsibilities within cyberspace. Recently, General Mark Welsh, USAF Chief of Staff, stated in a speech to the Air Force Association, that he is unsure of the requirements and what kind of expertise is needed for the cyberspace mission which could become a black hole.[78] Despite this uncertainty, increasing numbers of STEM educated personnel must be brought into the USAF. The challenge is to build and maintain a credible and competent Cyber ISR workforce. Given the

outlook for scarce resources and educated manpower, STEM growth in ISR must be an urgent priority for the USAF.

Recommendations for Further Research

The DoD rarely discloses the details of ISR operations. More research is needed at classified levels to understand the current tactics, techniques and procedures (TTPs) employed by cyber professional who provide decision makers with indications and warning. STEM educated Airmen are able to more effectively and efficiently employ our classified TTPs. More research is also needed to determine the exact requirements for STEM educated Airmen in specific Cyber ISR positions such as planners, collection managers, HUMINT agents and target officers. Finally, better monitoring and oversight of the USAF career field structure is needed. Recently, the US Navy realigned five ISR related career fields and created the Information-Dominance Corps, a restricted-line cadre of officers.[79] Rather than artificially separating communities, this new career path will combine the right skills and talents to dominate in the future.[80] The USAF has implemented the crew concept for cyber operations which may signal the first step to a further merger. Computer and intelligence personnel represent two of the most critical fields that deal with a blend of communications, intelligence, engineering, network defense, network operations, information operations and other specialties.[81] Who better poised for these challenges than STEM educated Airmen?

Endnotes:

[1] Joseph S. Nye, Jr., "Cyber Power", Harvard Kennedy School: Belfer Center for Science and International Affairs, (May 2010): 1-23. http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html

[2] Department of Defense. *Strategy for Operating in Cyberspace,* Washington, DC: Office of the Secretary of Defense, July 2011, 5.

[3] *AFDD-1: Air Force Basic Doctrine, Organization, and Command.* Washington, DC: LeMay Center, 14 October 2011, 1.
[4] Kamal T. Jabbour, "Cyber Vision and Cyber Force Development", *Strategic Studies Quarterly*: (Spring 2010), 64.
[5] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, (As Amended Through 15 August 2012), 156.
[6] Sebastian M. Convertino, et. al, *Flying and Fighting in Cyberspace*. Air University: Air University Press, 2007, 44.
[7] Kamal T. Jabbour, "50 Cyber Questions Every Airman Can Answer", *Wright-Patterson Public Affairs*: Air Force Research Laboratory (May 2008), 20.
[8] Mark M. Lowenthal, *Intelligence, From Secrets to Policy*, (CQ Press: 2012), 21.
[9] Kamal T. Jabbour, "Cyber Vision and Cyber Force Development", *Strategic Studies Quarterly*: (Spring 2010), 68.
[10] IBID.,71
[11] Walter D. Givhan, et al. "The Criticality of Defense-Focused Technical Education", *Air & Space Journal*: (Summer 2011): 16.
[12] IBID., 13.
[13] The United States Air Force. *14N Career Field Management Update*, Washington DC: Pentagon, AF/A2DFM, May 2012, 8-9.
[14] IBID., 8-9.
[15] Joseph S. Nye, Jr., "Cyber Power", Harvard Kennedy School: Belfer Center for Science and International Affairs, (May 2010): 3.
http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html
[16] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* (Santa Monica, CA: RAND, 2009), 11.
[17] Eric Sterner. "Retaliatory Deterrence in Cyberspace", Strategic Studies Quarterly, Vol. 5, no. 1 (Spring 2011), 64.
[18] Stephen W. Korns, "Cyber Operations: The New Balance", *Joint Force Quarterly*, Issue 54 (July 2009): 99.
[19] Thomas C. Wingfield, "International Law and Information Operations", *Cyber Power and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, National Defense University Press, 2009): 541.
[20] The White House, *The National Security Strategy of the United States of America*, (Washington, DC: US Government Printing Office, May 2010), 9.
[21] Department of Defense. *Strategy for Operating in Cyberspace,* Washington, DC: Office of the Secretary of Defense, July 2011, 11.
[22] Department of Defense. *Science, Technology, Engineering and Mathematics: STEM Education & Outreach Strategic Plan*, Washington, DC: Office of the Secretary of Defense, STEM Development Office, Dec 2009, 2.
[23] Larry K. McKee and Jim Ed Crouch. *Cyberspace Education and Training*. (Smithfield, VA: National Security Cyberspace Institute, 6 July 2010), 1.
[24] Department of Defense. *Science, Technology, Engineering and Mathematics: STEM Education & Outreach Strategic Plan*, Washington, DC: Office of the Secretary of Defense, STEM Development Office, Dec 2009, 1.
[25] Department of Defense. *Strategy for Operating in Cyberspace,* Washington, DC: Office of the Secretary of Defense, July 2011, 11.

[26] Air Force Institute of Technology. Cyber Workforce Development, Wright-Patterson AFB: Center for Cyberspace Research, September 2012, 6.
[27] The United States Air Force, Chief Scientist. *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025,* Washington DC: SAF Public Affairs, 2012, 65.
[28] IBID., 65.
[29] Air Force Guidance Memorandum 36-03, *Cyberspace Professional Development Program*, 16 Dec 2011, 3.
[30] Air Force Space Command. *Cyberspace Force Development: Training & Education*, Colorado Springs, CO: Air Force Space Command, 2012, 1.
[31] The United States Air Force. *The Air Force Roadmap for the Development of Cyberspace Professionals*, Washington DC: Pentagon, AF/A3O, 13 Aug 2010, 8.
[32] Air Force Doctrine Directive 3-12, *Cyberspace Operations,* 15 July 2010, 23.
[33] Host, Pat, "Air Force Trying to Get Six Cyber Capabilities Designated as Weapons Systems", *Defense Daily*: Vol. 226, Issue 39 (29 Nov 2012), 1.
[34] The United States Air Force. *The Air Force Roadmap for the Development of Cyberspace Professionals*, Washington DC: Pentagon, AF/A3O, 13 Aug 2010, 5.
[35] IBID., 5.
[36] Air Force Instruction 14-128, *Air Force Service Cryptologic Component (SCC),* AF/A2R, 28 September 2010, 2.
[37] Larry D. James, "Airmen: Delivering Decision Advantage", *Air & Space Journal*: (November-December 2012): 6.
[38] IBID., 6.
[39] Fulghum, David, "Strategic Stagnation", *Aviation Week & Space Technology*: Vol.171, Issue 14 (12 October 2009): 1.
[40] Vautrinot, Suzanne M. "Improving Military Capabilities for Cyber Operations", *Presentation to the Subcommittee on Emerging Threats and Capabilities, House Armed Services Committee, US House of Representatives*, (Department of the Air Force, July 2012), 9.
[41] Air Force Space Command. *The United States Air Force Blueprint for Cyberspace*, Colorado Springs, CO: Air Force Space Command, 2 Nov 2009, 19.
[42] IBID., 19.
[43] The United States Air Force, Chief Scientist. *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025,* Washington DC: SAF Public Affairs, 2012, 66.
[44] The United States Air Force. *STEM and Bright Horizons Update Briefing*, Washington DC: Pentagon, SAF/AQR, May 2011, 20.
[45] Sebastian M. Convertino, et. al, *Flying and Fighting in Cyberspace*. Air University: Air University Press, 2007, 70.
[46] IBID, 70.
[47] The United States Air Force. *Bright Horizons: the Air Force STEM Strategic Roadmap*, Washington DC: Pentagon, SAF/AQR, 9 Dec 2010, 16.
[48] Walter D. Givhan, et al. "The Criticality of Defense-Focused Technical Education", *Air & Space Journal*: (Summer 2011): 14.
[49] Air Force Personnel Center. *2013 Advanced Academic Degree (AAD) and Special Experience*

Exchange Duties (SPEED) Selection Process Guide, San Antonio, TX: Air Force Personnel Center, 27 April 2012, 1-26.
[50] Air Force Institute of Technology. *Cyber Workforce Development*, Wright-Patterson AFB: Center for Cyberspace Research, September 2012, 1-21.
[51] Kamal T. Jabbour, "Cyber Vision and Cyber Force Development", *Strategic Studies Quarterly*: (Spring 2010), 68.
[52] Major Daniel J. Reisner. Intelligence Officer Course Flight Commander, 315th Training Squadron, Goodfellow AFB, TEX. To the author. Email. 31 January 2013.
[53] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* (Santa Monica, CA: RAND, 2009), 11-12.
[54] Eric Sterner. "Retaliatory Deterrence in Cyberspace", Strategic Studies Quarterly, Vol. 5, no. 1 (Spring 2011), 68. Kamal T. Jabbour, "50 Cyber Questions Every Airman Can Answer", *Wright-Patterson Public Affairs*: Air Force Research Laboratory (May 2008), 11-12.
[55] Martin C. Libicki, *Cyberdeterrence and Cyberwar.* (Santa Monica, CA: RAND, 2009), 31.
[56] Air Force Space Command. *The United States Air Force Blueprint for Cyberspace*, Colorado Springs, CO: Air Force Space Command, 2 Nov 2009, 3-4.
[57] The United States Air Force. *The Air Force Roadmap for the Development of Cyberspace Professionals*, Washington DC: Pentagon, AF/A3O, 13 Aug 2010, 13.
[58] The White House, *The National Security Strategy of the United States of America*, (Washington, DC: US Government Printing Office, May 2010), 27.
[59] Marc V. Schanz, "Building Better Cyberwarriors", *Air Force Magazine*: (September 2010), 54.
[60] William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power-Economic and Military.* (Tuscaloosa: The University of Alabama Press, 2009), 6.
[61] *AFDD-1: Air Force Basic Doctrine, Organization, and Command.* Washington, DC: LeMay Center, 14 October 2011, 18.
[62] Air Force Space Command. *Enabling Concept for Delivery of Space-Derived Intelligence, Surveillance and Reconnaissance Data/Information for Battlespace Awareness*, Colorado Springs, CO: Air Force Space Command, 8 July 2011, 24.
[63] Jon Kimminau. "A Culminating Point for Air Force Intelligence, Surveillance and Reconnaissance", Air & Space Journal: (November-December 2012): 120.
[64] Mary Ann Lawlor, "Air Arms Around Intelligence", Signal: Vol. 66, no. 10 (Jun 2012), 19-22.
[65] The United States Air Force. *14N Career Field Management Update*, Washington DC: Pentagon, AF/A2DFM, May 2012, 22.
[66] The United States Air Force. *AFSC 14NX Intelligence Officer: Career Field Education and Training Plan*, Washington DC: Pentagon, AF/A2, Feb 2013, 27.
[67] The United States Air Force. *14N Career Field Management Update*, Washington DC: Pentagon, AF/A2DFM, May 2012, 39.
[68] The United States Air Force. *14N Career Field Management Update*, Washington DC: Pentagon, AF/A2DFM, May 2012, 8-9.
[69] The United States Air Force, Chief Scientist. *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025,* Washington DC: SAF Public Affairs, 2012, 66.
[70] Matthew M. Hurley, "For and from Cyberspace", *Air & Space Power Journal*: (November-December 2012): 24.
[71] Sebastian M. Convertino, et. al, *Flying and Fighting in Cyberspace*. Air University: Air

University Press, 2007, 68.
[72] Walter D. Givhan, et al. "The Criticality of Defense-Focused Technical Education", *Air & Space Journal*: (Summer 2011): 17.
[73] The United States Air Force. *14N Career Field Management Update*, Washington DC: Pentagon, AF/A2DFM, May 2012, 21.
[74] IBID., 27.
[75] Kamal T. Jabbour, "Cyber Vision and Cyber Force Development", *Strategic Studies Quarterly*: (Spring 2010), 70.
[76] Department of Defense. *Science, Technology, Engineering and Mathematics: STEM Education & Outreach Strategic Plan*, Washington, DC: Office of the Secretary of Defense, STEM Development Office, Dec 2009, 9.
[77] The United States Air Force. *Bright Horizons: the Air Force STEM Strategic Roadmap*, Washington DC: Pentagon, SAF/AQR, 9 Dec 2010, 22.
[78] Mike Hoffman, "Cyber Security, an Air Force Punchline", Defensetech, 26 Sept 2012, http://defensetech.org/2012/09/26/cyber-security-an-air-force-punchline/ (assessed 29 January 2013)
[79] Brown, Nancy, et al. "Creating Cyber Warriors", *US Naval Institute Proceedings*: Vol. 138, Issue 10 (October 2012), 2.
[80] IBID., 2.
[81] Marc V. Schanz, "Building Better Cyberwarriors", *Air Force Magazine*: (September 2010), 51.

Bibliography

Air Force Doctrine Directive 1, *Air Force Basic Doctrine, Organization, and Command,* Lemay Center, 14 October 2011, 1-134.

Air Force Doctrine Directive 3-12, *Cyberspace Operations,* 15 July 2010, 1-53.

Air Force Instruction 14-128, *Air Force Service Cryptologic Component (SCC),* AF/A2R, 28 September 2010, 1-12.

Air Force Guidance Memorandum 36-03, *Cyberspace Professional Development Program*, 16 Dec 2011, 1-16.

Air Force Institute of Technology. *Cyber Workforce Development*, Wright-Patterson AFB: Center for Cyberspace Research, September 2012, 1-21.

Air Force Personnel Center. *2013 Advanced Academic Degree (AAD) and Special Experience Exchange Duties (SPEED) Selection Process Guide*, San Antonio, TX: Air Force Personnel Center, 27 April 2012, 1-26.

Air Force Policy Directive 10-17, *Cyberspace Operations*, 31 July 2012, 1-9.

Air Force Space Command. *Cyberspace Force Development: Training & Education,* Colorado Springs, CO: Air Force Space Command, 2012, 1.

Air Force Space Command. *Enabling Concept for Delivery of Space-Derived Intelligence, Surveillance and Reconnaissance Data/Information for Battlespace Awareness*, Colorado Springs, CO: Air Force Space Command, 8 July 2011, 1-34.

Air Force Space Command. *The United States Air Force Blueprint for Cyberspace*, Colorado Springs, CO: Air Force Space Command, 2 Nov 2009, 1-12.

Brown, Nancy, et al. "Creating Cyber Warriors", *US Naval Institute Proceedings*: Vol. 138, Issue 10 (October 2012),1-4.

Convertino, Sebastian M., et. al, *Flying and Fighting in Cyberspace*. Air University: Air University Press, 2007, 44-71.

Department of Defense. *Science, Technology, Engineering and Mathematics: STEM Education & Outreach Strategic Plan*, Washington, DC: Office of the Secretary of Defense, STEM Development Office, Dec 2009, 1-13.

Department of Defense. *Strategy for Operating in Cyberspace,* Washington, DC: Office of the Secretary of Defense, July 2011, 1-13.

Fulghum, David, "Hackers Versus Cyberwarriors", *Aviation Week & Space Technology*: Vol. 174, Issue 27 (7 July 2012): 1-3.

Fulghum, David, "Strategic Stagnation", *Aviation Week & Space Technology*: Vol. 171, Issue 14 (12 October 2009): 1.

Givhan, Walter, D., et al. "The Criticality of Defense-Focused Technical Education", *Air & Space Journal*: (Summer 2011): 12-18.

Hoffman, Mike, "Cyber Security, an Air Force Punchline", Defensetech, 26 Sept 2012, http://defensetech.org/2012/09/26/cyber-security-an-air-force-punchline/ (assessed 29 January 2013)

Host, Pat, "Air Force Trying to Get Six Cyber Capabilities Designated as Weapons Systems", *Defense Daily*: Vol. 226, Issue 39 (29 Nov 2012), 1-2.

Hurley, Matthew M., "For and from Cyberspace", *Air & Space Power Journal*: (November-December 2012): 12-33.

Jabbour, Kamal T., "Cyber Vision and Cyber Force Development", *Strategic Studies Quarterly*:

(Spring 2010), 63-73.
Jabbour, Kamal T., "50 Cyber Questions Every Airman Can Answer", *Wright-Patterson Public Affairs*: Air Force Research Laboratory (May 2008), 1-24.
James, Larry D., "Airmen: Delivering Decision Advantage", *Air & Space Journal*: (November-December 2012): 1-11.
Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, (As Amended Through 15 August 2012), 1-525.
Kimminau, Jon, "A Culminating Point for Air Force Intelligence, Surveillance and Reconnaissance", *Air & Space Journal*: (November-December 2012): 113-129.
Korns, Stephen, W., "Cyber Operations: The New Balance", *Joint Force Quarterly*, Issue 54 (July 2009): 97-102.
Lachow, Irving. "Cyber Terrorism: Menace or Myth?" *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, (2009): 437-464.
Larios, Erwin A., "Posturing US Air Force Intelligence to Better Support Operations Against Cyber Threats", *Air Command and Staff College*, Air University: Air University Press (14 December 2011), 1-26.
Lawlor, Mary Ann, "Air Arms Around Intelligence", Signal: Vol. 66, no. 10 (Jun 2012), 19-22.
Libicki, Martin C. *Crisis and Escalation in Cyberspace.* (Santa Monica, CA: RAND, 2012), 1-172.
Libicki, Martin C. *Cyberdeterrence and Cyberwar.* (Santa Monica, CA: RAND, 2009), 1-125.
Libicki, Martin C., "The Specter of Non-Obvious Warfare", *Strategic Studies Quarterly*, Vol. 6, no. 3 (Fall 2012): 88-101.
Lowenthal, Mark M. *Intelligence, From Secrets to Policy*, (CQ Press: 2012), 1-386.
McKee, Larry K. and Jim Ed Crouch. *Cyberspace Education and Training*. (Smithfield, VA: National Security Cyberspace Institute, 6 July 2010), 1-14.
Mitchell, William, *Winged Defense: The Development and Possibilities of Modern Air Power-Economic and Military.* (Tuscaloosa: The University of Alabama Press, 2009), 1-302.
Mudrinich, Erik M., "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem", *Air Force Law Review*: Vol. 68 rev. 167 (2012), Air Force Judge Advocate General School, 1-45.
Nye, Jr., Joseph S. "Cyber Power", Harvard Kennedy School: Belfer Center for Science and International Affairs, (May 2010): 1-23. http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html (assessed 7 January 2013)
Reisner, Daniel J. Intelligence Officer Course Flight Commander, 315th Training Squadron, Goodfellow AFB, TEX. To the author. Email. 31 January 2013.
Schanz, Marc V., "Building Better Cyberwarriors", *Air Force Magazine*: (September 2010), 50-54.
Sterner, Eric. "Retaliatory Deterrence in Cyberspace", Strategic Studies Quarterly, Vol. 5, no. 1 (Spring 2011), 62-80.
The United States Air Force. *AFSC 14NX Intelligence Officer: Career Field Education and Training Plan*, Washington DC: Pentagon, AF/A2, Feb 2013, 1-59.
The United States Air Force. *14N Career Field Management Update*, Washington DC: Pentagon, AF/A2DFM, May 2012, 1-79.

The United States Air Force. *STEM and Bright Horizons Update Briefing*, Washington DC: Pentagon, SAF/AQR, May 2011, 1-66.

The United States Air Force. *Bright Horizons: the Air Force STEM Strategic Roadmap*, Washington DC: Pentagon, SAF/AQR, 9 Dec 2010, 1-26.

The United States Air Force. *The Air Force Roadmap for the Development of Cyberspace Professionals*, Washington DC: Pentagon, AF/A3O, 13 Aug 2010, 1-27.

The United States Air Force, Chief Scientist. *Cyber Vision 2025: United States Air Force Cyberspace Science and Technology Vision 2012-2025,* Washington DC: SAF Public Affairs, 2012, 1-84.

The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, DC: US Government Printing Office, May 2010, 1-25.

The White House, *The National Security Strategy of the United States of America*, (Washington, DC: US Government Printing Office, May 2010), 1-52.

Vautrinot, Suzanne M. "Improving Military Capabilities for Cyber Operations", *Presentation to the Subcommittee on Emerging Threats and Capabilities, House Armed Services Committee, US House of Representatives*, (Department of the Air Force, July 2012), 1-14.

Wingfield, Thomas C., "International Law and Information Operations", *Cyber Power and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, National Defense University Press, 2009): 525-543.